

TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK



APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

IN THE MATTER OF THE SEARCH
OF A CERTAIN IPHONE 11 PRO

20-MJ-242

Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ ☒
Name: AUSA Michael W. Gibaldi
Firm Name: _____
Address: U.S. Attorney's Office, EDNY
271A Cadman Plaza East, Brooklyn NY 11201
Phone Number: (718) 254-6067
E-Mail Address: michael.gibaldi@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO ☒

If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: _____; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

March 10, 2020
DATE

SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____

Judge/Magistrate Judge: _____

Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: Brooklyn, NEW YORK
March 10, 2020

U.S. DISTRICT JUDGE/U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE March 10, 2020
DATE

SK:MWG
F.#2019R01511

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ONE BLACK AND GREEN IPHONE 11
PRO, MODEL: MWA92LL/A, SERIAL
NUMBER C39ZP5Y5N6XQ,
CURRENTLY LOCATED IN THE
EASTERN DISTRICT OF NEW YORK

TO BE FILED UNDER SEAL

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. 20-MJ-242

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, KIERAN KEENAGHAN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of one black and green iPhone 11 Pro, Model MWA92LL/A, Serial Number C39ZP5Y5N6XQ (the “DEVICE”), which is currently in law enforcement’s possession in this District, and the extraction from that property of electronically stored information described in Attachment B. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

2. I am a Detective and Task Force Officer assigned to the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) and the New York City Police Department (“NYPD”) Joint Robbery Task Force. I have been a Detective with the NYPD since 1999. I have been a Task Force Officer with the ATF/NYPD Joint Robbery Task

Force since 2014. I have been involved in the investigations of numerous cases involving Hobbs Act robberies and related firearms offenses. Through my training, education and experience, I have become familiar with the manner in which evidence of robberies are commonly stored and the manner in which fugitives hide, as well as the uses and capabilities of cellular phones. I have also participated in the execution of search warrants involving evidence of robberies, including searches of electronic devices.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1951 (Hobbs Act robbery and conspiracy to commit the same) and 924(c) (possessing and discharging a firearm during a crime of violence) have been committed by THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and other, unidentified individuals. There is also probable cause to believe that MARQUIS AIKEN is the user of the DEVICE. There is also probable cause to search the information pertaining to the DEVICE, further described in Attachment A, for evidence, instrumentalities, or fruits of these crimes, as further described in Attachment B.

PROBABLE CAUSE

5. The United States, including the ATF, is conducting a criminal investigation of THURMEN RISHER (“RISHER”), DARNELL LEONARD (“LEONARD”), MARQUIS AIKEN (“AIKEN”), and other individuals regarding a pattern

of armed robberies that occurred in Brooklyn, New York and elsewhere in or about and between September 2019 and January 2020.

6. The following robberies involving RISHER, LEONARD, and other individuals occurred in or about and between September 2019 and October 2019:

- a. On or about September 19, 2019, at approximately 1:00 p.m., an armed robbery occurred at a laundromat located at 673 Bushwick Avenue, Brooklyn, New York;
- b. On or about September 23, 2019, at approximately 3:00 p.m., an armed robbery occurred at a Metro PCS store located at 1805 Fulton Street, Brooklyn, New York;
- c. On or about September 27, 2019, at approximately 1:30 p.m., an armed robbery occurred at a T-Mobile store located at 5002 Kings Highway, Brooklyn, New York;
- d. On or about October 5, 2019, at approximately 2:50 p.m., an armed robbery occurred at a jewelry store located at 28 Graham Avenue, Brooklyn, New York;
- e. On or about October 19, 2019, at approximately 12:22 p.m., an armed robbery occurred at a jewelry store located at 9 Hanover Place, Brooklyn, New York;
- f. On or about October 21, 2019, at approximately 10:00 a.m., an armed robbery occurred at a jewelry store located at 863 Central Avenue, Dover, New Hampshire.

7. I have reviewed video surveillance depicting the above-described robberies. Video surveillance shows LEONARD at each of the above-described robberies and RISHER at the above-described robbery on September 19, 2019.

8. According to historical cell-site data, RISHER's cellular telephone was located within close proximity to each of the above-described robberies near the times of each above-described robbery, and LEONARD's cellular telephone was located within close proximity to the above-described robberies on September 23, October 5, October 19 and October 21, near the times of each robbery.¹

9. RISHER has been charged with one count of Hobbs Act robbery, in violation of 18 U.S.C. § 1951(a), and LEONARD has been charged with one count of Hobbs Act robbery conspiracy, in violation of 18 U.S.C. § 1951(a).

10. On January 14, 2020, the Honorable Ramon E. Reyes, Jr., United States Magistrate Judge, Eastern District of New York, issued an arrest warrant for LEONARD.

11. Law enforcement agents arrested LEONARD seven days later while he was in the midst of committing an additional robbery of a jewelry store at the corner of 37th Avenue and 74th Street in Queens, New York. LEONARD was wearing a neoprene mask, sunglasses, and a black hooded sweatshirt, and he was attempting to enter a black Nissan

¹ There is no historical cell-site data for LEONARD's cellular telephone at the times of the above-described robberies on September 19 and September 27; however, historical cell-site data for LEONARD's cellular telephone places his cellular telephone near the locations of those robberies approximately one hour after each robbery, which is consistent with LEONARD's presence at those robberies.

Maxima, New York license plate HFD6301 (the “Vehicle”). The Vehicle was parked near the corner of 37th Avenue and 74th Street with the engine running and with another individual in the driver’s seat. As LEONARD attempted to enter the Vehicle, law enforcement agents stopped and arrested LEONARD. At the time of his arrest, LEONARD had an empty laundry bag concealed under his jacket.

12. I stopped the individual in the driver’s seat and determined that he was MARQUIS AIKEN. Law enforcement then arrested AIKEN on an open arrest warrant for unrelated sex trafficking charges pending in the Supreme Court of the State of New York, New York County. AIKEN was holding the DEVICE in his hand when I stopped him, and I seized the DEVICE from AIKEN incident to arrest.

13. Law enforcement have since determined that the Vehicle resembles a black Nissan Maxima captured on video surveillance fleeing the scene of a jewelry store robbery at 141-18 Holly Avenue in Queens, New York on December 19, 2019. Video surveillance from inside that jewelry store depicts one of the robbers wearing a mask similar to the one worn by LEONARD in Dover, New Hampshire on October 21, 2019.

14. Following AIKEN’s arrest, law enforcement agents, including myself, advised AIKEN of his Miranda rights, and AIKEN waived his Miranda rights and agreed to speak with law enforcement. AIKEN stated, in sum and substance and in part, that: LEONARD is his uncle; LEONARD called AIKEN on the DEVICE early that morning and asked AIKEN to pick up him in Queens; and LEONARD sent by text message a GPS “pin” showing his location to the DEVICE.

15. Based upon my training and experience, I am aware that individuals engaged in armed robberies often use their cellular telephones to communicate through text

messages, other messaging applications, and voice calls with other co-conspirators. In addition, based on the facts of this investigation, individuals in this Hobbs Act robbery conspiracy involving RISHER, LEONARD, and AIKEN use their cellular telephones to communicate through messages, other messaging applications, and voice calls with other co-conspirators.

16. The DEVICE is currently in the lawful possession of the ATF. Upon AIKEN's arrest, the NYPD took custody of the DEVICE and transferred it to the custody of the New York County District Attorney's Office (the "Manhattan DA"). A New York State court signed a warrant to search the DEVICE for evidence of the above-mentioned sex trafficking charges. I have retrieved the DEVICE from the Manhattan DA, and the DEVICE is currently in the ATF's custody in this District.² In my training and experience, I know that the DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the DEVICE first came into the possession of law enforcement.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

² ATF agents initiated a search of the DEVICE based on the search warrant issued by the New York State court; however, after consulting with the prosecutor in this case, agents stopped that initial search in order to apply for this warrant. The agents did not seize any information from the DEVICE in the initial search, did not use any information from the initial search in furtherance of this investigation, and did not use any information from the initial search in this search warrant application.

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various

types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time,

combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the

Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

18. Based on my training, experience and research, I know that the DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the DEVICE.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the DEVICE. This information can sometimes be recovered with forensics tools.

20. Forensic evidence. As further described in Attachment B2, this application seeks permission to locate not only electronically stored information that might

serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information

necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for the DEVICE that I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

22. Manner of execution. Because the warrant for the DEVICE seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

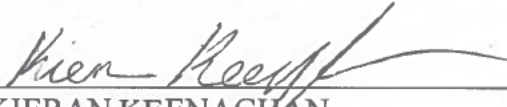
CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the DEVICE described in Attachment A to seek the items described in Attachment B.

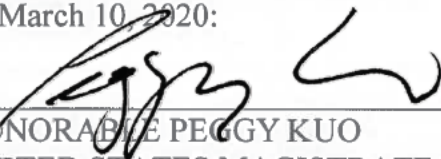
24. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the full extent of which

is neither public nor known to all of the targets of the investigation. Specifically, although RISHER and LEONARD have been apprehended, AIKEN has been released on bail in connection with the above-mentioned sex trafficking offense, and other co-conspirators remain unidentified and at large. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates and flee from prosecution.

Respectfully submitted,


KIERAN KEENAGHAN
Detective/Task Force Officer
NYPD/ATF Joint Robbery Task Force

Subscribed and sworn to before me by telephone
on March 10, 2020:


HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is one black and green iPhone 11 Pro, Model MWA92LL/A, Serial Number C39ZP5Y5N6XQ (the “DEVICE”). The DEVICE is currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and information on the DEVICE described in Attachment A that constitute fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1951 (Hobbs Act robbery and conspiracy to commit the same) and 924(c) (possessing and brandishing a firearm during a crime of violence) (collectively, the “SUBJECT OFFENSES”) involving THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and other, unidentified co-conspirators from September 1, 2019 to the present, including:

- a. Comments, communications, photographs and images concerning the SUBJECT OFFENSES;
- b. Associations and communications with and between THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and any other individuals involved in robberies with one or more of the foregoing individuals;
- c. Records of Internet activity concerning the SUBJECT OFFENSES, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- d. Evidence indicating the past locations of THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and any other individuals involved in robberies with one or more of the foregoing individuals;

- e. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited or deleted, such as logs, phonebooks, saved usernames and passwords, documents and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Hon. Peggy Kuo U.S.M.J.
Printed name and title

ReturnCase No.:
20-MJ-242

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

The property to be searched is one black and green iPhone 11 Pro, Model MWA92LL/A, Serial Number C39ZP5Y5N6XQ (the “DEVICE”). The DEVICE is currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records and information on the DEVICE described in Attachment A that constitute fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1951 (Hobbs Act robbery and conspiracy to commit the same) and 924(c) (possessing and brandishing a firearm during a crime of violence) (collectively, the “SUBJECT OFFENSES”) involving THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and other, unidentified co-conspirators from September 1, 2019 to the present, including:

- a. Comments, communications, photographs and images concerning the SUBJECT OFFENSES;
- b. Associations and communications with and between THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and any other individuals involved in robberies with one or more of the foregoing individuals;
- c. Records of Internet activity concerning the SUBJECT OFFENSES, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- d. Evidence indicating the past locations of THURMEN RISHER, DARNELL LEONARD, MARQUIS AIKEN, and any other individuals involved in robberies with one or more of the foregoing individuals;

- e. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited or deleted, such as logs, phonebooks, saved usernames and passwords, documents and browsing history.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.